# Data Protection Policy

**January 2017**

# Data Protection Policy

## Content

The Internet Business School collects and uses personal information about staff, students and other individuals who come into contact with the Internet Business School.

## 1.1 Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

## 2.1 Data Protection Principles

It is the duty of data controllers and data processors to comply with all the data protection principles. These are set out in Schedule 1 of the Data Protection Act 1998, from which the following extract is taken:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless —

(a) At least one of the conditions in Schedule 2 is met, and

(b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**General Statement**

The Internet Business School is committed to maintaining the above principles at all times. The Internet Business School will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

**3.1 Right of Access**

- Staff, students and other users of the University have the right to access personal data held about them by the University, whether in manual or electronic format.

- Any individual wishing to exercise this right should apply using the Subject Access

- Request form available from the Data Protection Co-ordinator.

- The Internet Business School will charge £10 per request.

**4. 1 Appendix 1**

**Subject Access Request**

1. Requests for information must be made in writing; which includes email, and be addressed to Internet Business School Director. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
    - passport
    - driving licence
    - utility bills with the current address
    - Birth / Marriage certificate
    - P45/P60
    - Credit Card or Mortgage statement

3. Any individual has the right of access to information held about them. However with

children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Director should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The response time for the subject access requests, once officially received is 40 working days. However the 40 days will not commence until after receipt of fees or clarification of information sought.

5. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

6. Third Party information is that which has been provided by another, such as the Police, Local Authority, Heath Care professional. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

7. If there are concerns over the disclosure of information then additional advice should be sought.

8. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

9. Information disclosed should be clear, any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

10. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

**5.1 Definitions**

**What is Data?**
Data means information:

- Stored in a form capable of being processed by computer [such as word-processed documents, spreadsheets and databases]

- Recorded in any form for later processing [such as registration forms, CCTV pictures]

- Stored as part of a ‘relevant filing system’. Note that this definition is very broad and covers such things as card indexes and microfiche files as well as traditional paper- based files. It

would be as well to assume that any paper-based data falls under the Act

**6.1 What is Personal Data?**

Personal data is defined as data that relates to a living individual who can be identified:

From that data; or

From data and other information in the possession of [or likely to come into the possession of] the Data Controller

And includes any expression of opinion about the individual and any indications of the intentions of the Data Controller or any other person in respect of that individual.

The Information Commissioner accepts this definition is 'not without difficulty'. It would always be safest to assume that data is personal rather than not.

**7.1 Sensitive personal data**

The 1998 Act distinguishes between ordinary "personal data" such as name, address and telephone number and "sensitive personal data" which includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive personal data is subject to much stricter conditions.

**8.1 Data Controller**

A 'Data Controller' is any person who makes decisions with regard to particular personal data, including decisions about the purposes for which the data is to be processed and the way in which that processing takes place. The Internet Business School is the Data Controller, but any member of staff may also be a Data Controller if he or she makes decisions about personal data and it's processing

**9.1 Complaints**

Complaints will be dealt with in accordance with the Internet Business School complaints policy. Complaints relating to information handling may be referred to the Information Commissioner.

**Section 10 Contact Information**

3.1 Your Internet Business School contact for this policy

If you have any queries about the contents of the policy, please contact our Customer Support team: Email: support@internetbusinessschool.com
Telephone:01233 226 222*
Post: Internet Business School, Bethersden, Ashford TN26 3EQ